CLAIMS

1. A method for providing security for a computer network, comprising:

generating content for a computer, wherein the computer is associated with the network;

determining whether a user should be routed to the generated content; and

routing the user to the generated content if it is determined that the user should be routed to the generated content.

2. The method of claim 1 further comprising monitoring the activities of the user with respect to the computer.

3. The method of claim 2 further comprising preventing the user from accessing files associated with said monitoring.

4. The method of claim 1 further comprising storing the packets sent by the user.

5. The method of claim 1 further comprising logging information concerning the files to which the user requests access.

6. The method of claim 1 further comprising preventing the user from accessing content within the computer other than the generated content.

7. The method of claim 1 further comprising screening a request by the user to access a file to determine if access is permitted.

8. The method of claim 7 further comprising permitting access to a requested file if it is determined that access to the requested file is permitted.

9. The method of claim 7 further comprising providing an indication that a requested file does not exist if it is determined that access is not permitted.

10. The method of claim 1 further comprising generating additional content subsequent to the step of generating content;

11. The method of claim 10 further comprising adding the additional content to the previously-generated content.

12. The method of claim 1 wherein the step of routing comprises using network address translation to route to the generated content any user that requests to access an unauthorized service.

13. The method of claim 12 wherein the unauthorized service is telnet.

14. The method of claim 1 further comprising receiving an indication that the user is no longer connected to the computer.

15. The method of claim 14 further comprising determining whether to retain changes in the files of the computer that resulted from the user's activities.

16. The method of claim 15 further comprising resetting the computer to restore the computer and the generated content to the condition they were in prior to the user being routed to the generated content if it is determined the changes should not be retained.

17. The method of claim 16 further comprising updating the generated content by generating additional content that appears to have been created during the time period during which the user was connected to the computer.

18. A method for providing security for a computer network, comprising:

generating content for a file system for a first computer associated with the network;

creating a directory within the first computer;

copying the file system of the first computer into the directory; and

routing a user who attempts to gain unauthorized access to a second computer associated with the network to the directory in the first computer.

19. The method of claim 18 further comprising generating operating system configuration information for the first computer.

20. The method of claim 18 further comprising copying the operating system of the first computer into the directory.

21. The method of claim 18 further comprising employing processes running outside of the directory to monitor the activities of the user within the directory.

22. The method of claim 21 further comprising screening requests by the user to access files to prevent the user from detecting the processes used to monitor the user.

23. A method for providing a virtual computer environment in a computer for test purposes, comprising:

creating a directory within the computer;

copying the file system of the computer into the directory; and

implementing a configuration change within the copy of the file system in the directory.

24. The method of claim 23 further comprising generating content for the file system.

25. The method of claim 23 further comprising making a copy of the file system after the configuration change has been implemented and resetting the virtual computer environment to the condition it was in before the configuration change was implemented.

26. The method of claim 25 further comprising comparing the copy of the file system after the configuration change has been implemented with the file system of the virtual

computer environment after it has been reset to determine the effect of the configuration change.

27. The method of claim 23 wherein the configuration change is the installation of a new software program.

28. The method of claim 23 wherein the configuration change is a change in the hardware installed on the computer.

29. The method of claim 23 wherein the configuration change is the connection of a new device to a network with which the computer is associated.

30. A system for providing security for a computer network, comprising:

a computer configured to generate content for the computer, wherein the computer is associated with the network; and

a network device configured to determine whether a user should be routed to the generated content and to route the user to the generated content if it is determined that the user should be routed to the generated content.

31. The system of claim 30, wherein the network device is a firewall.

32. A computer program product for providing security for a computer network, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

generating content for a computer, wherein the computer is associated with the network;

determining whether a user should be routed to the generated content; and

routing the user to the generated content if it is determined that the user should be routed to the generated content.